FORM PTO-1390 REV. 5-93 US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**	ATTORNEYS DOCKET NUMBER **P00,0622** U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/581359

INTERNATIONAL APPLICATION NO. **PCT/DE98/03545**	INTERNATIONAL FILING DATE **02 DECEMBER 1998**	PRIORITY DATE CLAIMED **18 DECEMBER 1997**

TITLE OF INVENTION
METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING SUBSCRIBERS

APPLICANT(S) FOR DO/EO/US
CHRISTIAN MENZEL ET AL.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)) - drawings attached.
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2) - drawings attached.

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report).**

12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**

13. ☒ Amendment "A" Prior to Action.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☒ Other items or information:
    a. ☒ Submission of Informal Drawings - 2 sheets of drawings, Figures 1-3; and
    Request for Approval of Drawing Modifications, Figures 1-3.

    b. ☒ EXPRESS MAIL #EL 544622965US dated June 9, 2000.

U.S. APPLICATION NO (if known, see 37 C.F.R. 1.5) 09/581359	INTERNATIONAL APPLICATION NO PCT/DE98/03545	ATTORNEY'S DOCKET NUMBER P00,0622

17. ☒ The following fees are submitted:

BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5):

Search Report has been prepared by the EPO or JPO $840.00

International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) . . $670.00

No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) $760.00

Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $970.00

International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . $ 96.00

				CALCULATIONS	PTO USE ONLY
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	15 - 20 =	0	X $ 18.00	$	
Independent Claims	02 - 3 =	0	X $ 78.00	$	
Multiple Dependent Claims			$260.00 +	$	
TOTAL OF ABOVE CALCULATIONS =				$ 840.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)				$	
SUBTOTAL =				$ 840.00	
Processing fee of $130.00 for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 840.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +					
TOTAL FEES ENCLOSED =				$ 840.00	
				Amount to be refunded	$
				charged	$

a. ☒ A check in the amount of $ 840.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. ____________ in the amount of $ ________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 08-2290. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Hill & Simpson
A Professional Corporation
85th Floor Sears Tower
Chicago, Illinois 60606

Steven H. Noll
SIGNATURE

Steven H. Noll
NAME

28,982
Registration Number

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	Christian Menzel et al.
ATTORNEY DOCKET NO.:	P00,0622
INTERNATIONAL APPLICATION NO:	PCT/DE98/03545
INTERNATIONAL FILING DATE:	02 December 1998

INVENTION: "METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING SUBSCRIBERS"

Assistant Commissioner for Patents,
Washington D.C. 20231

AMENDMENT "A" PRIOR TO ACTION

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE SPECIFICATION:

On page 1:

cancel lines 1-4 and substitute the following

--SPECIFICATION

TITLE

METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING SUBSCRIBERS"

BACKGROUND OF THE INVENTION

Field of the Invention-- therefor;

above line 9, insert

--Description of the Related Art--;

in line 9, cancel ", for example,";

in line 11, cancel "," and substitute --.-- therefor;

in line 12, cancel "connections" and substitute --Connections-- therefor;

in line 13, cancel "being capable of being" and substitute --can be-- therefor;

in line 14, cancel "said" and substitute --this-- therefor;

in line 17, cancel "The" and substitute --In this article, the-- therefor;

in line 18, cancel "thereby";

in line 19, cancel "means - also referred to as";

in line 20, cancel "or SIM card -" and substitute -- (SIM) card-- therefor;

in lines 21-22, cancel "means - for example,--;

in line 22, cancel "-";

in line 25, cancel "ensues" and substitute --takes place in a-- therefor, and after "related", insert --manner--;

in line 27, after "systems", insert --,--, and cancel ", for example,"; and

in line 29, cancel the first "the" and substitute --a--therefor.

On page 2:

in line 1, cancel "is thereby" and substitute --in these systems is-- therefor;

in lines 3-4, cancel "etc., in contrast whereto" and substitute --. By contrast,-- therefor;

in line 11, cancel ", this" and substitute --. This is-- therefor, cancel "being", and cancel "in" and substitute --for-- therefor;

in line 12, after "given", insert --a--;

above line 14, insert

--SUMMARY OF THE INVENTION--;

in lines 16-17, cancel "so that" and substitute --enabling--therefor;

in line 17, cancel "derives";

cancel lines 18-21 and substitute the following therefor

-- This object is inventively achieved by a method for encryption of information for a radio transmission and for authentication of subscribers in a communication system that comprises an access network having equipment for the radio transmission, the communication system further comprising at least one core network having a respective authentication equipment for the subscriber authentication, the method comprising the steps of allocating a radio channel for the transmission of the information via a radio interface from/to at least one base station of the access network, mutually transmitting public keys between a mobile station and the base station via the radio interface, encrypting subsequent information to be transmitted via the radio interface using one of the public keys received by the base station or the mobile station, deciphering encrypted information received by the mobile station or the base station on the basis of a private key that is allocated to the transmitted, public key in the mobile station or in the base station, and authenticating the core network via a subscriber identity mobile card of the mobile station, and authenticating the subscribers via the authentication equipment of the core network on the basis of encrypted information that have been mutually sent.

This object is also achieved by a communication system for encryption of information for a radio transmission and for authentication of, comprising an access network having equipment for the radio transmission as well as at least one core network, the core network having a respective authentication equipment for the subscriber authentication, the communication system utilizing a radio channel for transmission of the information via a radio interface from/to at least one base station of the access network, memory devices in a mobile station and in the base station for storing public keys and private keys that are allocated to the public keys, transmitters in the mobile station and in the base station for mutually sending the public keys via the radio interface, controllers in the mobile station and in the base station for encryption of the information to be subsequently sent via the radio interface upon employment of the public keys received by the base station or, respectively, the mobile station and for deciphering the received, encrypted information on the basis of the stored, appertaining private key the mobile station comprising a subscriber identity mobile card for authenticating the core network, the core network comprising an authentication equipment for authenticating the subscribers; and the authenticating the core network and the authenticating the subscribers utilizing mutually transmitted, encrypted information.--

in lines 27-28, cancel “, respectively,” and substitute --the-- therefor;

in line 30, cancel “, respectively,” and substitute --the-- therefor; and

in line 32, cancel “, respectively,”.

On page 3:

in line 2, cancel “means” and substitute --component/equipment-- therefor;

in line 3, cancel “the means” and substitute --a component/equipment-- therefor;

in line 7, cancel “ensue” and substitute --take place in a-- therefor;

in line 8, after both instances of “related”, insert --manner--, and after “of”, insert --a--;

in line 12, cancel the first “-“ and substitute --(-- therefor, and cancel the second “-“ and substitute --)-- therefor;

in line 13, cancel “,” and substitute --(-- therefor, and after “authentication”, insert --)--;

in line 16, cancel “this having not been” and substitute --which was not-- therefor;

in line 27, cancel “means” and substitute --device-- therefor; and

in line 30, cancel “means” and substitute --device-- therefor.

On page 4:

in lines 2-3, cancel “, that latter using this” and substitute --which uses this key-- therefor;

in line 22, cancel “means of the”;

in line 25, cancel “ensues” and substitute --occurs-- therefor;

in lines 25-26, cancel “, this being capable of being” and substitute --which can be-- therefor;

in line 26, after “implemented”, insert --,--, and cancel “given” and substitute --for-- therefor;

in line 28, cancel “means of the”;l

in line 30, cancel “means from the”; and

in line 31, cancel “the means of” therefor.

On page 5:

in line 2, cancel “network means” and substitute --core network-- therefor;

in line 3, cancel “network means” and substitute --core network-- therefor;

in line 6, cancel “means”;

in line 9, cancel “see to” and substitute --implement-- therefor;

in line 13, cancel “, respectively,”;

in line 16, cancel “means” and substitute --authentication mechanism-- therefor;

in line 17, cancel “control means” and substitute --controller-- therefor;

above line 20, insert

--BRIEF DESCRIPTION OF THE DRAWINGS --;

cancel line 22;

in line 23, cancel “the” and substitute --is a-- therefor;

in line 26, cancel “the message” and substitute --is a message--, and after “flow”, insert --diagram--;

in line 29, cancel “the message” and substitute --is a message--, and after “flow”, insert --diagram--; and

in lines 30-31, cancel “a network means of”.

On page 6:

above line 1, insert

--DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

in line 1, after “a”, insert --universal network--;

in line 2, cancel “, for example,”;

in line 6, cancel “, for example,”;

in line 7, cancel “thereto - is thereby” and substitute --to it - is-- therefor;

in line 11, cancel “, for example,”;

in line 16, cancel “means” and substitute --authentication equipment-- therefor; and

in line 28, cancel “thereby”.

On page 7:

in line 3, after “have”, insert --a--;

in line 4, cancel “means”;

in line 5, cancel “transmission and reception means” and substitute --transmitter and receiver-- therefor;

in lines 6-7, cancel “transmission and reception means” and substitute --transmitter and receiver-- therefor;

in line 7, cancel the first “means”, and cancel “transmission and reception means” and substitute --transmitter and receiver-- therefor;

in lines 8-9, cancel “control means” and substitute --controller-- therefor;

in line 9, cancel the “means” after “memory”;

in lines 9-10, cancel “transmission and reception means” and substitute --transmitter and receiver-- therefor;

in lines 11-12, cancel “- station-related via the transmission and reception means MSE -”;

in line 15, cancel the first “means” and cancel “control means” and substitute --controller-- therefor;

in line 19, cancel “means” and substitute --entity-- therefor, and after “i.e.”, insert --,--;

in line 20, cancel “It” and substitute --The base station-- therefor;

in line 23, cancel the first “means”, and cancel “control means” and substitute --controller-- therefor;

in line 25, cancel “these begin” and substitute --which are-- therefor;

cancel line 27 and substitute --station BS or its controller BST-- therefor;

in line 30, cancel “-“ and substitute --,-- therefor; and

in line 31, cancel “-“.

On page 8:

in line 4, cancel “[..]” and substitute --method-- therefor, and cancel “thereby” and substitute --thus-- therefor;

in line 5, cancel “of” and substitute --in-- therefor;

in line 9, cancel “transmission and reception means” and substitute --transmitter and receiver-- therefor;

in line 10, cancel “, said first public key PUK1-BS having” and substitute --which has-- therefor;

in line 11, cancel “being” and cancel “control means” and substitute --controller-- therefor;

in line 12, cancel “means”;

in line 13, cancel “following”, and after “information”, insert --that follows it--;

in line 19, cancel “listen to this” and substitute --eavesdrop-- therefor;

in line 22, cancel “means” and substitute -- subscriber identity mobile card-- therefor, and after “authentication”, insert --,--;

in lines 22-23, cancel “controller means”;

in line 25, cancel “means” and substitute --authentication equipment--

therefor;

in line 30, cancel “means” and substitute --entity-- therefor; and

in line 31, cancel “means” and substitute --entity-- therefor, and cancel “as”.

On page 9:

in line 3, cancel “comprised thereof”;

in line 5, before “signed”, insert --and--;

in line 8, cancel “-“ and substitute --,--;

in line 9, cancel “-“;

in line 14, cancel “Further” and substitute --Furthermore-- therefor, and before “access”, insert --the--;

in line 15, before “core”, insert --the--;

in line 16, cancel “wherein” and substitute --in which-- therefor;

in line 20, cancel “The example” and substitute --This example-- therefor; and

in line 21, cancel “thereby limited thereto” and substitute --limited in-- therefor.

On page 10:

in line 10, before “third”, insert --and--;

in line 11, cancel “not being” and substitute --are not-- therefor, and cancel “into”;

in line 14, cancel “thereby”;

in line 17, cancel “being” and substitute --and are-- therefor;

in line 18, cancel “thereof” and substitute --of it-- therefor;

in lines 20-21, cancel “-specific means” and substitute --identity mobile card-- therefor;

in lines 21-22, cancel “- on the basis of the subscriber-related SIM card-“;

in line 22, cancel “means” and substitute --authentication equipment--

therefor;

in line 24, cancel "thereby ensues" and substitute --takes place in--, and after "encrypted", insert --format--;

in line 25, cancel "means" and substitute --authentication equipment-- therefor;

in line 29, cancel "means" and substitute --authentication equipment-- therefor;

in line 31, cancel "thereto"; and

in line 32, cancel "means" and substitute --authentication equipment-- therefor.

On page 11:

in line 1, cancel ", said means" and substitute --. The authentication equipment-- therefor, and cancel "implementing" and substitute --implements-- therefor;

in line 2, cancel "- likewise" and substitute --in a likewise manner-- therefor;

in line 6, cancel "ensues" and substitute --takes place-- therefor;

in line 7, cancel "-specific means (SIN)" and substitute --identity mobile card (SIM)--;

in line 8, cancel "network means" and substitute --authentication equipment-- therefor;

in line 10, cancel "-" and substitute --,-- therefor;

in line 13, after "achieved", insert --.--;

in line 14, cancel "and access", and substitute --The access-- therefor, cancel the first "-" and substitute --(-- therefor, and cancel "- and" and substitute --) and the-- therefor;

in line 15, cancel the first "-" and substitute --(-- therefor, and cancel "the second "-" and substitute --)-- therefor; and below line 16, insert

-- The above-described method and communication system are illustrative of the principles of the present invention. Numerous modifications and adaptions thereof will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.--.

IN THE CLAIMS:

On page 12, line 1, replace "**PATENT CLAIMS**" with --WHAT IS CLAIMED IS:--

Please amend claims 1-15 as follows:

1. (Amended) A method [Method] for encryption of information for a radio transmission and for authentication of subscribers [(S1, S2)] in a communication system [(UNM),] that [-] comprises an access network [(ACN)] having equipment [(BS, BSC)] for said [the] radio transmission, said communication system further comprising a [as well as at least one] core network [(CON1, CON2)] having a respective authentication equipment [(AC, AC=)] for said [the] subscriber authentication, comprising the steps of:

[- allocates] allocating a radio channel [(RCH)] for said [the] transmission of said [the] information via a radio interface [(AI)] from/to a [at least one] base station [(BS)] of said [the] access network; [(ACN), whereby]

[-] mutually transmitting public keys [(PUK1-MT, PUK-BS) are mutually transmitted] between a mobile station [(MT)] and said [the] base station [(BS)] via said [the] radio interface; [(AI),]

[-] encrypting subsequent information to be transmitted via said radio interface using one of said [the] public keys [key (PUK1-MT or, respectively, PUK-BS)] received by said [the] base station [(BS)] or [, respectively,] said mobile station; [(MT) is employed for encryption of the information to be subsequently transmitted via the radio interface (AI),]

[- the] deciphering encrypted information received by said [the] mobile station [(MT)] or [, respectively,] said base station [(BS) are deciphered] on the basis of a private key [(PRK1-MT, PRK1-BS)] that is allocated to said [the] transmitted, public key [(PUK1-MT, PUK-BS)] in said [the] mobile station [(MT)] or [, respectively,] in said [the] base station; and [(BS), and whereby]

[-] authenticating said core network via a subscriber identity mobile card [-specific means (SIN)] of said [the] mobile station [(MT) implements the authentication of the respective core network (CON1, CON2)], and authenticating said subscribers via said authentication equipment [the means (AC, AC=)] of said [the] core network [(CON1, CON2) implements the authentication of the subscriber (S1, S2)] on the basis of encrypted information that have been mutually sent.

2. (Amended) A method [Method] according to claim 1, further comprising the steps of: [whereby]

[-] sending a first public key [(PUK1-MT) is first sent] from said [the] mobile station [(MT)] to said [the] base station; [(BS),]

encrypting [which employs it for the encryption of the] information to be sent to said [by the] mobile station [(MT)] using said first public key by said base station;

[- a] sending an other public key [(PUK-BS) is sent] from said [the] base station [(BS)] to said [the] mobile station; [(MT),]

encrypting [which employs it for the encryption of the] information to be sent to said [the] base station [(BS)] using said other public key by said mobile station, and; [and, subsequently,]

[- the mobile station (MT) sends] sending a second public key [(PUK2-MT)] to said [the] base station [(BS)] by said mobile station subsequent to said step of sending said other public key from said base station.

3. (Amended) A method [Method] according to claim 2, further comprising the step of replacing said first [whereby the second] public key [(PUK2-MT) replaces the first] with said second public key [(PUK1-MT)] sent to said [the] base station [(BS)].

4. (Amended) A method [Method] according to claim 1, further comprising the steps of: [whereby

- the base station (BS) first sends a first public key (PUK1-BS) to the mobile station (MT) that employs for encryption of the information to be sent to the base station (BS);

- the mobile station (MT) sends a public key (PUK-MT) to the base station (BS) that employs for the encryption of the information to be sent to the mobile station (MT); and, subsequently,

- the base station (BS) sends a second public key (PUK2-BS) to the mobile station (MT).]

sending a first public key from said base station to said mobile system;

encrypting information to be sent to said base station using said first public key by said mobile station;

sending an other public key from said mobile station to said base station;

encrypting information to be sent to said mobile station using said other public key by said mobile station; and

sending a second public key to said mobile station by said base station subsequent to said step of sending said other public key from said mobile station.

5. (Amended) A method [Method] according to claim 4, further comprising the step of replacing said first [whereby the second] public key [(PUK2-BS) replaces the first] with said second public key [(PUK1-BS)] sent to said [the] base station [(BS)].

6. (Amended) A method [Method] according to claim 1, further comprising the steps of: [one of the preceding claims, whereby]

[- the mobile station (MT) sends] sending a subscriber identity [(SID)] of said [the] subscriber [(S1, S2)] and an authentication request [(aureq-mt)] by said mobile station to said [the] core network [(CON1, CON2)] in encrypted form; [, and]

returning, by said authenticating equipment [the means (AC, AC=)] of the core network, [(CON1, CON2) returns] an authentication reply [(aures-co)] in encrypted form; and

[- the] implementing, by said mobile station, [(MT) implements] an authentication procedure for checking an [the] identity of said [the] core network [(CON1, CON2)].

7. (Amended) A method [Method] according to claim 6, further comprising the steps of: [whereby]

[- the means (AC, AC=) of the core network (CON1, CON2) sends] sending an authentication request [(aureq-co)] in addition to said [the] authentication reply (aures-co) in encrypted form by said authenticating equipment of said core network; [, and]

returning, by said [the] mobile station, [(MT) returns] an authentication reply [(aures-mt)] to said authenticating equipment of said core network [the means (AC)] in encrypted form; and

[- the means (AC, AC=) implements] checking said subscriber identity by an authentication procedure implemented by said authenticating equipment of said core network [for checking the subscriber identity (SID)].

8. (Amended) A method [Method] according to claim 1, further comprising the step of implementing said authentication procedure utilizing [one of the preceding claims, whereby] secret keys [(ki) are employed for the authentication procedure].

9. (Amended) A method [Method] according to claim 1, further comprising the steps of: [one of the preceding claims, whereby]

servicing, by said [the] access network [(ACN) services] at least two core networks [(CON1, CON2)] in parallel; and

registering and authenticating in different core networks, a subscriber [one or more subscribers (S1, S2)] that can use said [the] mobile station [(MT)] in parallel [are registered and authenticated in different core networks (CON1, CON2)].

10. (Amended) A method [Method] according to claim 1, further comprising the step of: [one of the claims 1 through 8, whereby the]

servicing, by access network, [(ACN) services] a core network [(CON)] in which a plurality of subscribers [(S1, S2)] that can use said [the] mobile station [(MT)] in parallel are registered and authenticated.

11. (Amended) A method [Method] according to claim 1, wherein said [one of the preceding claims, whereby the] access network [(ACN)] and said [the] core network or multiple core networks [(CON1, CON2)] are administered by different network operators.

12. (Amended) A communication [Communication] system for encryption of information for a radio transmission and for authentication of subscribers [(S1, S2)], comprising:

[-] an access network [(ACN)] having equipment [(BS, BSC)] for said [the] radio transmission as well as a [at least one] core network [(CON1, CON2)], said core network having a respective authentication equipment [means (AC, AC=)] for said [the] subscriber authentication, said communication system utilizing [-] a radio channel [(RCH)] for transmission of said information [the intervention] via a radio interface [(AI)] from/to a [at least one] base station [(BS)] of the access network; [(ACN),

and comprising]

[-] memory devices [(MSP, BSP)] in a mobile station [(MT)] and in said [the] base station [(BS)] for storing public keys [(PUK1-MT, PUK-BS)] and private keys [PRK1-BS, PRK1-BS [sic])] that are allocated to said [the] public keys [(PUK1-MT, PUK-BS)],

[- transmission devices (MSE, BSE)] transmitters in said [the] mobile station [(MT)] and in said [the] base station [(BS)] for mutually sending said [the] public keys [(PUK1-MT, PUK1-BS)] via said [the] radio interface; [(AI),]

[- control devices (MST, BST)] controllers in said [the] mobile station [(MT)] and in said [the] base station [(BS)] for encryption of said [the] information to be subsequently sent via said [the] radio interface [(A1)] upon employment of said [the] public keys [(PUK1-MT or, respectively, PUK-BS)] received by said [the] base station [(BS)] or, respectively, said mobile station [(MT)] and for deciphering [the] received, encrypted information on the basis of said [the] stored, appertaining private key [(PRK1-MT, PRK1-BS), and]

said mobile station comprising [-] a subscriber identity mobile card [-specific means (SIN) in the mobile station (MT) and a means (AC, AC=) in the respective core network (CON1, CON2)] for authenticating said [the implementation of the authentication of the] core network; [(CON1, CON2) as well as]

said core network comprising an authentication equipment for authenticating said [the authentication of the] subscribers; and [(S1, S2)]

said authenticating said core network and said authenticating said subscribers utilizing [on the basis of] mutually transmitted, encrypted information.

13. (Amended) A communication [Communication] system according to claim 12, wherein said [comprising an] access network [(ACN) to which] has at least two core networks [(CON1, CON2) are] connected in parallel for [the] registration and authentication of a subscriber [one or more subscribers (S1, S2)] that can use said [the] mobile station [(MT)] in parallel in different core network

[(CON1, CON2)].

14. (Amended) A communication [Communication] system according to claim 12, wherein said [comprising an] access network [(ACN) to which] has a core network [(CON1) is] connected for [the] registration and authentication of a plurality of subscribers [(S1, S2)] that can use said [the] mobile station [(MT)] in parallel.

15. (Amended) A communication [Communication] system according to claim 12 [one of the preceding claims, comprising an] wherein said access network [(ACN)] and said core network or multiple core networks are administered by [one or more core networks (CON1, CON2) that exhibit] different network operators.

IN THE ABSTRACT

On page 17:

cancel lines 2-3;

in line 9, cancel ", respectively,";

in line 10, cancel ", respectively,";

in line 13, cancel ", respectively,";

in line 15, cancel ", respectively,";

in line 16, cancel "mobile radio telephone-specific means (SIN)" and substitute --subscriber identity mobile card (SIM)-- therefor;

in line 18, cancel "a means" and substitute --authentication equipment-- therefor; and

cancel line 21.

REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment of claims 1-15 is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

Steven H. Noll (Reg. No. 28,982)

Steven H. Noll
Hill & Simpson
A Professional Corporation
85th Floor - Sears Tower
Chicago, Illinois 60606
(312) 876-0200
Attorney for Applicant(s)

2 | PART

SPECIFICATION

METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING OF SUBSCRIBERS

The invention is directed to a method for the encryption of information for a radio transmission and for authentication of subscribers in a communication system and is also directed to a corresponding communication system.

Communication systems such as, for example, the mobile radio telephone system according to the GSM standard (global system for mobile communication) use a radio interface for wireless information transmission, connections between mobile stations and base stations of a mobile radio telephone network being capable of being setup, released and maintained on said radio interface. A method and a system for encryption (ciphering) information for radio transmission and for subscriber authentication are known from the article “Safety First bei europaweiter Mobilkommunikation”, telcom report 16 (1993), No. 6, pages 326 through 329. The mobile subscribers thereby identify themselves with respect to the mobile radio telephone network using a means - also referred to as subscriber identity mobile or SIM card - that is contained in the radio telephone subscriber station. At the network side, the mobile subscriber is registered in a means - for example, an authentication means (authentication center) - that respectively offers security parameters and security algorithms for the protection of the subscriber data of the mobile subscribers. The encryption of the information on the radio interface ensues subscriber-related and is directly coupled to the subscriber authentication.

In future communication systems such as, for example, a universal network (UMTS, universal mobile telecommunication system or UPT, universal personal communication), there is the tendency to divide the infrastructure into an access network and into one or more core networks.

The area of the access network is thereby responsible for matters of the radio interface such as administration and allocation of the radio channels, channel encoding, encryption via the radio interface, etc., in contrast whereto the area of the core network is mainly responsible for matters of the subscriber administration such as registration (subscription), authentication, selection of the access network, etc., as well as for offering services. An encryption of the information for the radio transmission independently of the core network is impossible in the current GSM system. Over and above this, a radio resource, for example the radio channel, is exclusively used for only one subscriber in the encryption, namely the subscriber that was authenticated at the moment, this no longer being adequate in future communication systems, particularly given simultaneous use of a mobile station by a plurality of subscribers (for example, with their SIM cards).

The invention is based on the object of specifying a method and a communication system that enables an encryption of the information at the radio interface independently of the nature and plurality of core networks, so that a functional separation of encryption and authentication derives.

This object is inventively achieved by the method comprising the features of patent claim 1 and by the communication system comprising the features of patent claim 12. Developments of the invention can be derived from the subclaims.

The subject matter of the invention proceeds from an encryption of the information for the radio transmission in an access network as well as from an authentication in at least one core network. Inventively, public keys are transmitted in alternation between a mobile station that can be used in parallel by a plurality of subscribers and the base station, being sent via the radio interface, and the public key received by the base station or, respectively, mobile station is employed for the encryption of the information to be subsequently transmitted via the radio interface. The encrypted information received by the mobile station or, respectively, base station can be deciphered on the basis of a private key that is allocated in the mobile station or, respectively, in the base station to the public key that was transmitted. Following the deciphering procedure, the authentication of the respective core network is implemented by a means of the mobile station, and the authentication of the subscriber is implemented by the means of the core network on the basis of the encrypted information transmitted in alternation.

As a result of the mutual transmission of public keys between mobile station and base station, the encryption for the radio transmission can ensue mobile station-related instead of subscriber-related and, thus, can simultaneously ensue for a plurality of subscribers. There is a bidirectional, trusted relationship into which an "apparent" base station or an unauthorized base station cannot intervene. Another advantage is the functional separation of access network - responsible for encryption - and core network, responsible for authentication. The radio resource is multiply utilized for the encryption of a plurality of subscribers at the mobile station. The information required for the authentication procedure can already be transmitted encrypted, this having not been possible in the previous GSM system. Maximum security is achieved by the combination of the encryption with public/private keys at the mobile station level and the following authentication at the subscriber level. In particular, a plurality of core networks - potentially of different network types - can be connected parallel to the access network due to the functional separation of access network and core network, and, in particular, a plurality of subscribers having different identities (SIM cards) can communicate simultaneously via a mobile station and in different core networks.

No third party can subsequently sneak into the secure connection, achieved by multiple, mutual transmission of the public keys. The following authentication assures that the respective partner means of the connection - i.e., the base station from the point of view of the mobile station or, respectively, the mobile station from the point of view of the base station - is also in fact the means that it pretended to be at the beginning of the communication.

An advantageous development of the invention provides that the mobile station first sends a first public key to the base station, that latter using this for the encryption of the information, and a public key is sent from the base station to the mobile station that employs it for the encryption of the information. Subsequently, the mobile station sends a second public key to the base station. The involvement of an "apparent" base station or of the unauthorized base station into the connection is thus dependably prevented at the radio interface. The second key thereby preferably replaces the first key.

According to an alternative development of the invention, the base station first sends a first public key to the mobile station, which employs it for encryption of the information, and the mobile station sends a public key to the base station, which employs it for the encryption of the information. Subsequently, the base station sends a second public key to the mobile station. The involvement of the "apparent" base station or of the unauthorized base station in the connection is thus dependably prevented at the radio interface. The second key is thereby preferably replaced by the first key.

It is advantageous according to another development of the invention that the mobile station sends a subscriber identity of the subscriber and an authentication request to the core network in encrypted form and receives an authentication reply from the means of the core network sent back to it in encrypted form. Subsequently, the mobile station implements an authentication procedure for checking the identity of the core network. A network authentication thus ensues at the side of the mobile station, this being capable of being individually implemented particularly given a plurality of core networks dependent on where the subscriber is registered.

The means of the core network preferably sends an authentication request in addition to the authentication reply in encrypted fashion, and an authentication reply is sent back to the means from the mobile station in encrypted form. Subsequently, the means of the core network can implement an authentication procedure for checking the subscriber identity.

This has the advantage that the request for checking the subscriber authentication can be co-transmitted with the reply of the network means to the network authentication and can be initiated by the network means immediately upon arrival of the reply.

A communication system according to the invention comprises memory means as a mobile station that can be used in parallel by a plurality of subscribers and of the base station for storing public keys and private keys that are allocated to the public keys. Transmission devices in the mobile station and in the base station see to the mutual transmission of the public keys via the radio interface. Control devices in the mobile station and in the base station are provided for the encryption of the information to be subsequently transmitted via the radio interface upon employment of the public key received from the base station or, respectively, mobile station and for deciphering the received, encrypted information on the basis of the stored, appertaining private key. Over and above this, the communication system comprises a subscriber-specific means in the mobile station and a control means in the respective core network for the implementation of the authentication of the core network as well as of the authentication of the subscribers on the basis of mutually transmitted, encrypted information.

The invention is explained in greater detail below on the basis of an exemplary embodiment with reference to the graphic illustration.

Thereby shown are:

FIG. 1 the block circuit diagram of a communication system with an access network for the radio transmission and a plurality of core networks for the authentication;

FIG. 2 the message flow for the encryption of the information at the radio interface between a mobile station and a base station of the access network; and

FIG. 3 the message flow for the authentication of the subscribers and of the core networks between the mobile station and a network means of the respective core network.

The communication system show in FIG. 1 is a communication system UNW - such as, for example, a universal UMTS or UPT network (universal mobile telecommunication system or universal personal telecommunication) - whose infrastructure is divided into an access network ACN and into one or more core networks CON1, CON2. The area of the access network ACN having devices of a radio sub-system - such as, for example, base stations BS and base station controllers BSC connected thereto - is thereby responsible for matters of the radio interface such as administration and allocation of radio channels, channel encoding, encryption via the radio interface, etc. The area of the core network CON1, CON2 with network equipment - such as, for example, switching equipment MSC, MSC' and authentication equipment AC, AC' - is mainly responsible for matters of routing, of subscriber administration such as registration (subscription) of the subscribers S1, S2 as well as authentication, selection of the access network ACN, etc., and for offering services. The authentication procedures in the means AC, AC' preferably use secret keys ki according to the known procedure of the GSM standard in order to implement the subscriber authentication for the subscriber S1 registered in the core network CON1 and for the subscriber S2 registered in the core network CON2 in parallel and independently of the access network ACN.

In the present example, the switching equipment MSC, MSC' in the core networks CON1 and CON2 are connected to the base station controller BSC of the access network ACN. The base station controller BSC enables the connection to at least one base station, to the base station BS in the present example. Such a base station BS is a radio station that is provided for coverage of a radio area - for example, of a radio cell - in order to setup, release and maintain connections from/to at least one mobile station MT that resides in its radio area via radio interface AI. The information are thereby contained in a radio channel RCH allocated by the base station controller BSC. The connections can be a matter of outgoing connections as well as of incoming connections. The mobile station MT in the present example is especially suited for simultaneous use by a plurality of subscribers S1 and

S2 that are attached in parallel to an internal bus (not shown) on the basis of their subscriber-specific devices SIM (subscriber identity module) and each have respectively separate subscriber identity.

The mobile station MT comprises a memory means MSP, a transmission and reception means MSE as well as control devices MST, MST' that are connected to the memory means MSP and transmission and reception means MSE. Likewise, the base station BS comprises a memory means BSP, a transmission and reception means BSE as well as a control means BST that is connected to the memory means BSP and transmission and reception means BSE.

According to the invention, the mobile station MT - station-related via the transmission and reception means MSE - sends a first public key PUK1-MT via the radio interface AI in parallel for all subscribers active at it and makes note of an appertaining, private key PRK1-MT that is deposited in the memory means MSP or in the control means MST. The base station BS employs the received, public key PUK1-MT for the encryption of the information to be subsequently sent via the radio interface AI. The deciphering of the information sent by the base station BS is thus only possible for the means that knows the appertaining private key, i.e. the mobile station MT with the key PRK1-MT. It in turn sends a public PUK-BS in the reply of the base station BS in the opposite direction to the mobile station MT and makes note of the appertaining private key PRK1-BS. The memory means BSP or the control means BST stores the private key PRK1-BS. It is thus assured that information subsequently sent by the mobile station MT to the base station BS, these being encrypted upon employment of the public key PUK1-BS, can only in turn be deciphered by the base station BS or, respectively, the control means BST thereof.

In order to prevent an “apparent” base station or unauthorized base station from using the public key PUK1-MT communicated from the mobile station MS for sending correctly encrypted information - arbitrarily or intentionally -, the mobile station MT sends a second public key PUK2-MT (already encrypted) to the base station BS via the radio interface AI. This key PUK2-MT can only be read and employed by the correct base station BS with which a trusted relationship was initially set up on the mobile station level. The "apparent" base station or unauthorized base station is dependably suppressed in this [..]. The second public key PUK2-MT thereby replaces the previous, first public key PUK1-MT. The same is true of the other transmission direction when the mutual transmission of the keys was initiated by the base station BS.

The encryption procedure can likewise be initiated by the base station BS, so that the transmission and reception means BSE sends a first public key PUK1-BS to the mobile station MT, said first public key PUK1-BS having a private key PRK1-BS allocated to it and being stored in the control means BST or in the memory means BSP. The mobile station MT employs the arriving, public key PUK1-BS for encryption of the following information and in turn sends a public key PUK-MT to the base station BS that employs it for the encryption of the information in the opposite direction. Subsequently, the base station BS preferably sends a second public key PUK2-BS to the mobile station MT in order to be absolutely certain that an undesired base station does not mix itself into the encrypted information transmission via the radio channel or listen to this. The public as well as the private keys are composed, for example, of a numerical sequence or bit sequence.

Following the encryption procedure, the mobile station MT - preferably, the means SIM provided only for the authentication or a control means MST responsible in common for encryption and authentication - implements the authentication of the respective core network CON1, CON2, and the means AC, AC' of the core network CON1, CON2 implements the authentication of the subscriber S1, S2 on the basis of mutually transmitted, encrypted information at the subscriber level (see Fig. 3). The bidirectional authentication is thus implemented independently of the access network ACN. The authentication appended to the encryption offers maximum security since it assures that the cooperating means of the connection is in fact the means that it identified itself as at the beginning of the communication. This prevents the overall communication on this connection from having been initiated by an “apparent” base station or unauthorized base station. Another advantage of the functional separation of encryption and authentication is comprised thereof that the subscriber identities and the information required for the authentication - for example, random number RAND, signed response SRES according to a GSM method - can already be transmitted encrypted via the radio interface AI. Authentication procedures deviating from GSM methods can also be employed for the authentication.

A plurality of core networks - the two core networks CON1, CON2 in the present example -, even if different network types, can be connected parallel to the access network ACN. The subscribers S1, S2 simultaneously work with different SIM cards via the one mobile station MT in different core networks - in the two core networks CON1, CON2 in the present example - or, respectively, one or more subscribers S1, S2 work in a single core network, for example CON1. Further, the functional separation of access network ACN and core network CON1, CON2 also supports configurations wherein the access network ACN and the core network or networks CON1, CON2 exhibit different network operators.

In a schematic illustration, FIG. 2 shows the message flow for encryption of the information for the radio transmission between the mobile station MT and the base station BS of the access network. The example is thereby limited thereto that the mutual exchange of the keys is initiated by the mobile statio MT. The base station BS could likewise begin the exchange (also see the description for FIG. 1); the following message flow would then be executed in a corresponding way.

After the allocation of the radio channel RCH for a connection setup for communication, the mobile station MT starts the encryption in that it transmits the public key PUK1-MT in a message SEND and makes note of the appertaining, private key PRK1-MT. The encrypted transmission of the information has thus begun at the radio interface. The base station BS uses the arriving key PUK1-MT for encrypted information transmission in the opposite direction, and in turn transmits the public key PUK-BS in the message SEND. It also makes note of the private key PRK1-BS belonging to the public key PUK-BS. The information transmitted in encrypted form - at least the public key PUK-BS in the present case - can only be deciphered by the mobile station MT with the assistance of the private key PRK1-MT that is only known to it. After the deciphering, the mobile station MT sends a second public key PUK-MT to the base station BS in a further message SEND, this base station BS deciphering the arriving information - at least the second public key PUK2-MT in the present case - with the assistance of the private key PRK1-BS that is only known to it. The second public key PUK2-MT thereby replaces the previous, first public key PUK1-MT. A trusted relationship has thus been produced between the two devices, third parties not being capable of penetrating into this relationship.

In a schematic illustration, FIG. 3 shows the message flow for authentication of the subscribers S1, S2 registered in different core networks and for authentication of the respective core network. Messages are thereby transmitted between the subscribers S1, S2 using the mobile station MT and the network equipment AC, AC' (authentication center) of the respective core network, being transmitted transparently for the access network and the base station thereof.

First, the subscriber S1 or, respectively, the mobile station MT transmits an authentication request aureq-mt via the subscriber-specific means (SIM) for the subscriber and a subscriber identity SID - on the basis of the subscriber-related SIM card - in the message SEND to the means AC of the core network responsible for the subscriber S1. The transmission of the information thereby ensues encrypted. In the opposite direction, the means AC returns an authentication reply aures-co in the message SEND to the mobile station MT that implements the authentication procedure - with, preferably, a secret key - for checking the authentication for the core network. With the authentication reply aures-co, an authentication request aureq-co is preferably simultaneously co-transmitted from the means AC of the core network in encrypted form and is received by the mobile station MT. In response thereto, the mobile station returns an authentication reply aures-mt in the message SEND to the means AC in encrypted form and subscriber-related, said means AC implementing the authentication procedure for checking the subscriber authentication - likewise, preferably, upon employment of secret keys. An authentication in only one direction - i.e., only for the subscribers or for the network - is also fundamentally possible.

The executive sequence for the authentication of the subscriber S2 ensues in a corresponding way by exchanging messages SEND having the above contents between the corresponding, subscriber-specific means (SIN) of the mobile station MT and the network means AC' of the other core network responsible for it. As a result of the combination of encryption at the radio interface from/to the access network - achieved on the basis of repeatedly exchanged public keys on the mobile station level, and following the authentication using secret keys on the subscriber level from/to the core network independently of the access network, maximum security is achieved and access network - responsible for the encryption - and core network or networks - responsible for authentication - nonetheless remain functionally separate.

PATENT CLAIMS

1. Method for encryption of information for a radio transmission and for authentication of subscribers (S1, S2) in a communication system (UNM), that

- comprises an access network (ACN) having equipment (BS, BSC) for the radio transmission as well as at least one core network (CON1, CON2) having a respective equipment (AC, AC') for the subscriber authentication,
- allocates a radio channel (RCH) for the transmission of the information via a radio interface (AI) from/to at least one base station (BS) of the access network (ACN),

whereby

- public keys (PUK1-MT, PUK-BS) are mutually transmitted between a mobile station (MT) and the base station (BS) via the radio interface (AI),
- the public key (PUK1-MT or, respectively, PUK-BS) received by the base station (BS) or, respectively, mobile station (MT) is employed for encryption of the information to be subsequently transmitted via the radio interface (AI),
- the encrypted information received by the mobile station (MT) or, respectively, base station (BS) are deciphered on the basis of a private key (PRK1-MT, PRK1-BS) that is allocated to the transmitted, public key (PUK1-MT, PUK-BS) in the mobile station (MT) or, respectively, in the base station (BS), and whereby
- a subscriber-specific means (SIN) of the mobile station (MT) implements the authentication of the respective core network (CON1, CON2), and the means (AC, AC') of the core network (CON1, CON2) implements the authentication of the subscriber (S1, S2) on the basis of encrypted information that have been mutually sent.

2. Method according to claim 1, whereby

- a first public key (PUK1-MT) is first sent from the mobile station (MT) to the base station (BS), which employs it for the encryption of the information to be sent by the mobile station (MT);
- a public key (PUK-BS) is sent from the base station (BS) to the mobile station (MT), which employs it for the encryption of the information to be sent to the base station (BS); and, subsequently,
- the mobile station (MT) sends a second public key (PUK2-MT) to the base station (BS).

3. Method according to claim 2, whereby the second public key (PUK2-MT) replaces the first key (PUK1-MT) sent to the base station (BS).

4. Method according to claim 1, whereby

- the base station (BS) first sends a first public key (PUK1-BS) to the mobile station (MT) that employs for encryption of the information to be sent to the base station (BS);
- the mobile station (MT) sends a public key (PUK-MT) to the base station (BS) that employs for the encryption of the information to be sent to the mobile station (MT); and, subsequently,
- the base station (BS) sends a second public key (PUK2-BS) to the mobile station (MT).

5. Method according to claim 4, whereby the second public key (PUK2-BS) replaces the first key (PUK1-BS) sent to the base station (BS).

6. Method according to one of the preceding claims, whereby
- the mobile station (MT) sends a subscriber identity (SID) of the subscriber (S1, S2) and an authentication request (aureq-mt) to the core network (CON1, CON2) in encrypted form, and the means (AC, AC') of the core network (CON1, CON2) returns an authentication reply (aures-co) in encrypted form;
- the mobile station (MT) implements an authentication procedure for checking the identity of the core network (CON1, CON2).

7. Method according to claim 6, whereby
- the means (AC, AC') of the core network (CON1, CON2) sends an authentication request (aureq-co) in addition to the authentication reply (aures-co) in encrypted form, and the mobile station (MT) returns an authentication reply (aures-mt) to the means (AC) in encrypted form;
- the means (AC, AC') implements an authentication procedure for checking the subscriber identity (SID).

8. Method according to one of the preceding claims, whereby secret keys (ki) are employed for the authentication procedure.

9. Method according to one of the preceding claims, whereby the access network (ACN) services at least two core networks (CON1, CON2) in parallel and one or more subscribers (S1, S2) that can use the mobile station (MT) in parallel are registered and authenticated in different core networks (CON1, CON2).

10. Method according to one of the claims 1 through 8, whereby the access network (ACN) services a core network (CON) in which a plurality of subscribers (S1, S2) that can use the mobile station (MT) in parallel are registered and authenticated.

11. Method according to one of the preceding claims, whereby the access network (ACN) an the core network or networks (CON1, CON2) are administered by different network operators.

12. Communication system for encryption of information for a radio transmission and for authentication of subscribers (S1, S2), comprising

- an access network (ACN) having equipment (BS, BSC) for the radio transmission as well as at least one core network (CON1, CON2) having a respective means (AC, AC') for the subscriber authentication,
- a radio channel (RCH) for transmission of the intervention via a radio interface (AI) from/to at least one base station (BS) of the access network (ACN),

and comprising

- memory devices (MSP, BSP) in a mobile station (MT) and in the base station (BS) for storing public keys (PUK1-MT, PUK-BS) and private keys PRK1-BS, PRK1-BS [sic]) that are allocated to the public keys (PUK1-MT, PUK-BS),
- transmission devices (MSE, BSE) in the mobile station (MT) and in the base station (BS) for mutually sending the public keys (PUK1-MT, PUK1-BS) via the radio interface (AI),
- control devices (MST, BST) in the mobile station (MT) and in the base station (BS) for encryption of the information to be subsequently sent via the radio interface (A1) upon employment of the public keys (PUK1-MT or, respectively, PUK-BS) received by the base station (BS) or, respectively, mobile station (MT) and for deciphering the received, encrypted information on the basis of the stored, appertaining private key (PRK1-MT, PRK1-BS),

and comprising

- a subscriber-specific means (SIN) in the mobile station (MT) and a means (AC, AC') in the respective core network (CON1, CON2) for the implementation of the authentication of the core network (CON1, CON2) as well as for the authentication of the subscribers (S1, S2) on the basis of mutually transmitted, encrypted information.

13. Communication system according to claim 12, comprising an access network (ACN) to which at least two core networks (CON1, CON2) are connected in parallel for the registration and authentication of one or more subscribers (S1, S2) that can use the mobile station (MT) in parallel in different core network (CON1, CON2).

14. Communication system according to claim 12, comprising an access network (ACN) to which a core network (CON1) is connected for the registration and authentication of a plurality of subscribers (S1, S2) that can use the mobile station (MT) in parallel.

15. Communication system according to one of the preceding claims, comprising an access network (ACN) and one or more core networks (CON1, CON2) that exhibit different network operators.

ABSTRACT

Method and Communications System for Ciphering Information for a Radio Transmission and for Authenticating of Subscribers

The subject matter of the invention proceeds from an encryption of the information for the radio transmission in an access network (ACN) as well as an authentication in at least one core network (CON1, CON2). Inventively, public keys (PUK1-MT, PUK-BS) are mutually transmitted between a mobile station (MT) and the base station (BS) via the radio interface (AI), and the public key (PUK1-MT or, respectively, PUK-BS) received by the base station (BS) or, respectively, mobile station (MT) is employed for the encryption of the information to be subsequently sent via the radio interface. On the basis of a private key (PRK1-MT, PRK1-BS) that is allocated to the transmitted, public key (PUK1-MT, PUK-BS) in the mobile station (MT) or, respectively, in the base station (BS), the encrypted information received by the mobile station or, respectively, base station can be deciphered. Following the encryption procedure, a mobile radio telephone-specific means (SIN) of the mobile station implements the authentication of the respective core network (CON1, CON2), and a means (AC, AC') of the core network implements the authentication of the subscriber on the basis of the mutually transmitted, encrypted information.

FIG. 1

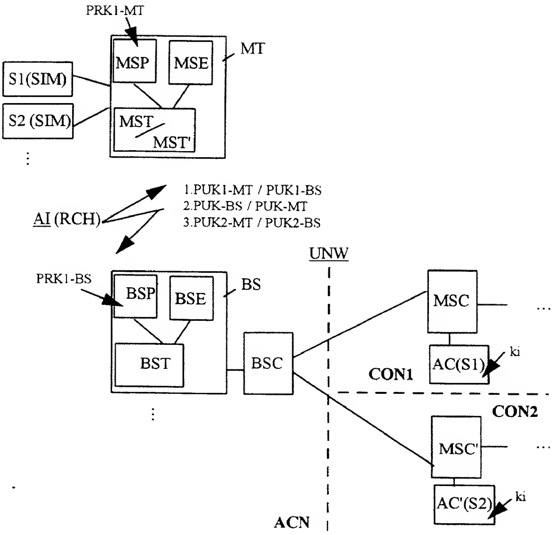
PRK1-MT
MSP
MSE
MT
S1(SIM)
S2 (SIM)
MST
MST'
AI (RCH)
1.PUK1-MT / PUK1-BS
2.PUK-BS / PUK-MT
3.PUK2-MT / PUK2-BS
UNW
PRK1-BS
BSP
BSE
BS
BST
BSC
MSC
...
AC(S1)
ki
CON1
CON2
MSC'
...
AC'(S2)
ki
ACN

Figure 1

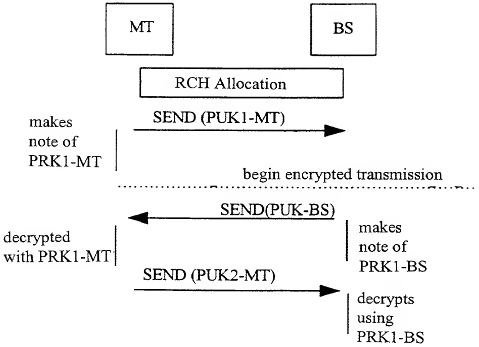

Figure 2

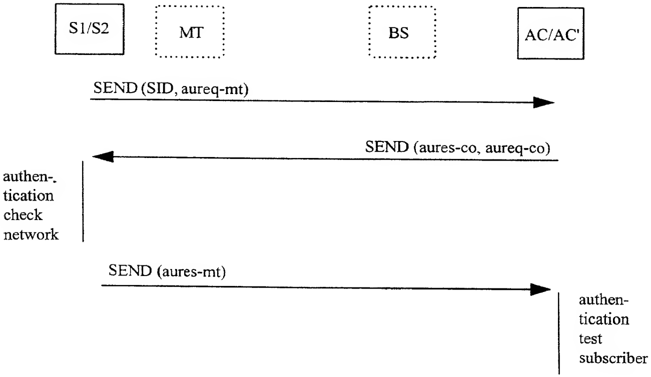
S1/S2
MT
BS
AC/AC'
SEND (SID, aureq-mt)
SEND (aures-co, aureq-co)
authen-. tication check network
SEND (aures-mt)
authen- tication test subscriber

Figure 3

Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgefuhrt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren und Kommunikationssystem zur Verschlüsselung von Informationen für eine Funkübertragung und zur Authentifikation von Teilnehmern

deren Beschreibung

(zutreffendes ankreuzen)

☒ hier beigefügt ist.

□ am ____________________ als

PCT internationale Anmeldung

PCT Anmeldungsnummer ____________________

eingereicht wurde und am ____________________

abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

____

____

____

____

the specification of which

(check one)

□ is attached hereto

□ was filed on ____________________ as

PCT international application

PCT Application No. ____________________

and was amended on ____________________

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Priorität beansprucht

Priority Claimed

197 56 587.5	Germany	18. Dezember 1997	☒ Yes Ja	□ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)		
			□ Yes Ja	□ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)		
			□ Yes Ja	□ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eıngereicht)		

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*	POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Messrs. John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

(19)

Telefongespräche bitte richten an: *(Name und Telefonnummer)*	Direct Telephone Calls to: *(name and telephone number)* 312/876-0200 Ext. ________________

Postanschrift:	Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

1-00

Voller Name des einzigen oder ursprünglichen Erfinders: MENZEL, Christian	Full name of sole or first inventor:
Unterschrift des Erfinders Datum X X 27.11.98	Inventor's signature Date
Wohnsitz D-82216 Maisach, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Edelweißstr. 36	Post Office Address
D-82216 Maisach Bundesrepublik Deutschland	
Voller Name des zweiten Miterfinders (falls zutreffend): HAFERBECK, Ralf	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum X X 30.11.98	Second Inventor's signature Date
Wohnsitz D-85716 Unterschleißheim, GERMANY DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift St.-Benedikt-Str. 5	Post Office Address
D-85716 Unterschleißheim Bundesrepublik Deutschland	

2-00

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).	*(Supply similar information and signature for third and subsequent joint inventors).*